Automation for System Safety Analysis: Technical Presentation

Jane T. Malin

Abstract This presentation describes work to integrate a set of tools to support early model-based analysis of failures and hazards due to system-software interactions. The tools perform and assist analysts in the following tasks: 1) extract model parts from text for architecture and safety/hazard models; 2) combine the parts with library information to develop the models for visualization and analysis; 3) perform graph analysis and simulation to identify and evaluate possible paths from hazard sources to vulnerable entities and functions, in nominal and anomalous system-software configurations and scenarios; and 4) identify resulting candidate scenarios for software integration testing. There has been significant technical progress in model extraction from Orion program text sources, architecture model derivation (components and connections) and documentation of extraction sources. Models have been derived from Internal Interface Requirements Documents (IIRDs) and FMEA documents. Linguistic text processing is used to extract model parts and relationships, and the Aerospace Ontology also aids automated model development from the extracted information. Visualizations of these models assist analysts in requirements overview and in checking consistency and completeness.

Automation for System Safety Analysis

Technical Presentation

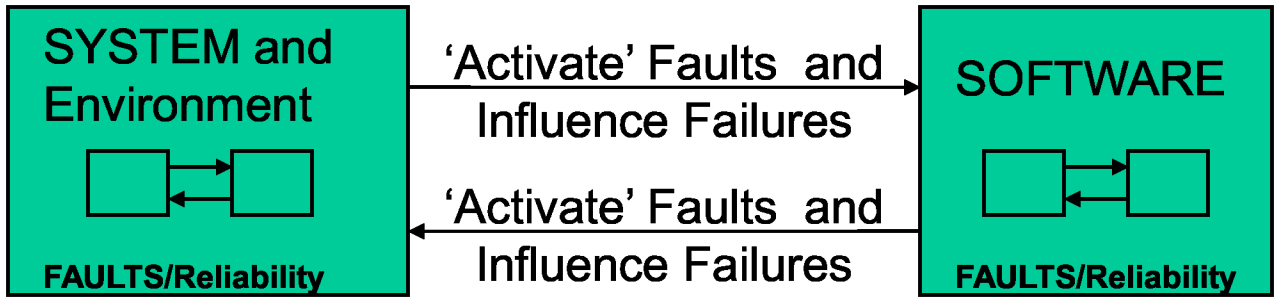
Project:
Automated Tool and Method for System Safety Analysis

Jane T. Malin, Principal Investigator
NASA JSC Team: Land Fleming, David Throop, Carroll Thronesbery, and summer intern Joshua Flores
Triakis Team: Ted Bennett and Paul Wennberg

Software Assurance Symposium 2009

Problem

- NASA needs early evaluation of software-system integration risks and constraints
  - Assess system faults, failures and hazards that may challenge software in system integration testing
  - Identify robustness and safety issues early
  - Identify requirements gaps early
- Process of reviewing various large and uncoordinated source documents is difficult

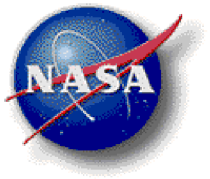


Approach and Relevance

- Semi-automated modeling for Safety Analysis and to identify cases for Integration Testing:
  Documents → Extract Text → Construct Model and Visualization → Analyze Hazard Paths and Simulate
  - Focus on system integration, interfaces, failures and hazards, which cause most of aerospace software (requirements) defects
  - Focus on information from Preliminary Design Review (PDR) – benefit of early analysis is greatest
    - Two Constellation Crew Exploration Vehicle (CEV) cases
      - Launch Abort System (LAS) pyrotechnics and Crew Module (CM)
      - Service Model (SM) propulsion

Summary of Products

- Models constructed from information extracted from text documents
- Visualizations for insight into information scattered in large documents
- Component model templates
- Output for model reuse



Latest Results

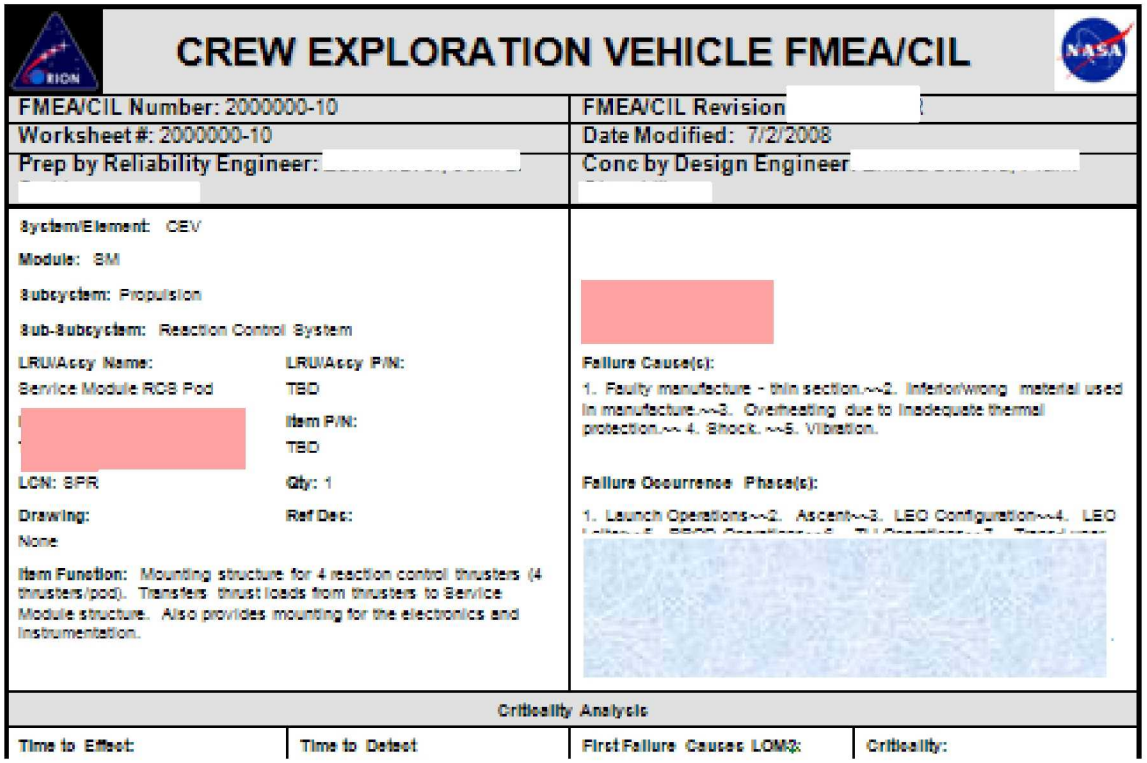
- Model Information Extraction from Text
  - Variety of types of documents analyzed
  - Variety of information types extracted
- Model Construction
  - Component-Connection Models and Visualizations
  - Model templates for path analysis

Overview of Method and Tools

- Develop system connection model and visualization
  - Acquire PDR-level documents
    - Interface requirements, failure modes and effects analyses, hazard reports
  - Automatically extract needed model information
    - Document analysis and linguistic analysis
  - Semi-automatically construct model, visualization and traceability information
    - Nomenclature ontology and component templates library
- Export the information for reuse
- Perform path analysis and simulation to analyze potential hazard paths

Source Documents and Cases

- Documents
  - Failure Mode and Effects Analysis/Critical Items List (FMEA/CIL)
  - Internal Interface Requirements Document (IIRD)
  - Hazard Reports
- Challenges
  - Variety of Formats
  - Document Maturity
  - Quality of the data



CREW EXPLORATION VEHICLE FMEA/CIL

FMEA/CIL Number: 2000000-10	FMEA/CIL Revision
Worksheet #: 2000000-10	Date Modified: 7/2/2008
Prep by Reliability Engineer:	Conc by Design Engineer

System/Element: CEV
Module: SM
Subsystem: Propulsion
Sub-Subsystem: Reaction Control System
LRU/Assy Name: Service Module RCS Pod
LRU/Assy P/N: TBD
Item P/N: TBD
LCN: SPR
Qty: 1
Drawing: None
Ref Des:
Item Function: Mounting structure for 4 reaction control thrusters (4 thrusters/pod). Transfers thrust loads from thrusters to Service Module structure. Also provides mounting for the electronics and instrumentation.

Failure Cause(s):
1. Faulty manufacture - thin section.~~2. Inferior/wrong material used in manufacture.~~3. Overheating due to inadequate thermal protection.~~ 4. Shock. ~~5. Vibration.

Failure Occurrence Phase(s):
1. Launch Operations~~2. Ascent~~3. LEO Configuration~~4. LEO

Criticality Analysis

Time to Effect:	Time to Detect	First Failure Causes LOM?:	Criticality:

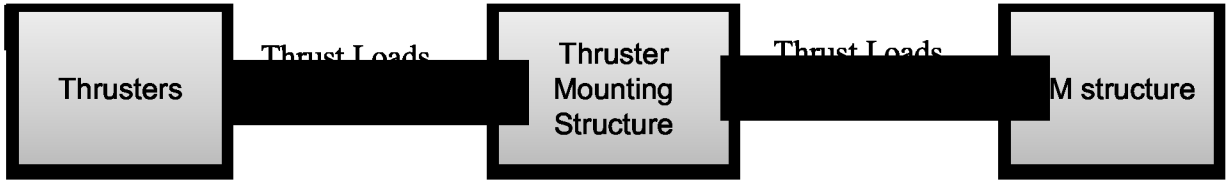
FMEA/CIL Worksheet for Thruster Mounting Structure

Semantic Text Analysis Tool (STAT) Extractions

- System to subcomponent indentured hierarchy
  - From FMEA/CIL document front matter section organization
  - From FMEA/CIL worksheet hierarchy: System/Element, Module, Subsystem, Sub-Subsystem
  - From FMEA/CIL worksheet failure modes and cause description: Item subcomponents
  - From Hazard Report cause descriptions and cause controls
- Components, connections and connection content
  - From IIRDs: Provide and receive statements
  - From FMEA/CIL worksheet Item function description: Provide, receive, transfer statements
  - From sensor names, e.g., “Flange Temperature Sensor”
- Function, failure and phase Information
  - From IIRDs: Item vulnerabilities and limits, operational context
  - From FMEA/CIL worksheet: item functions/actions, failure mode description, cause description, mission phase
  - From Hazard Report causes descriptions and cause controls
- Acronyms
- Traceability Information: Source document and source texts

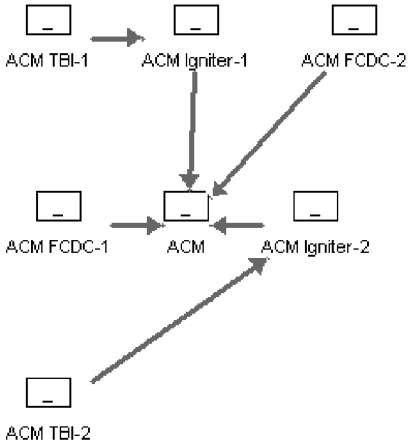
Linguistic Extraction Progress

- Approach: Parse words and phrases in document text
  - Specify relevant sections and fields for analysis, using document structure grammar
  - After linguistic analysis, use Aerospace Ontology nomenclature to identify phrases that indicate problems and verbs that indicate
    - Actions/Functions
    - Connecting relationships – e.g., sends, supplies, transfers, distributes, carries
    - Part-of or other structural relationships – contains, consists of, comprises
  - XML-formatted output of relevant model information
- Progress
  - Extraction from multiple document data structures and mime types
    - General format specification approach
  - Better linguistic analysis for information extraction
    - Integrated advanced parser from University of Central Florida

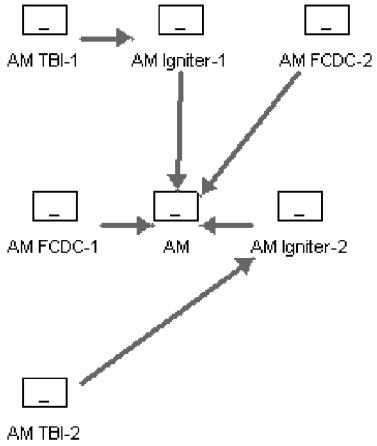


LAS Pyro Visualization from FMEA

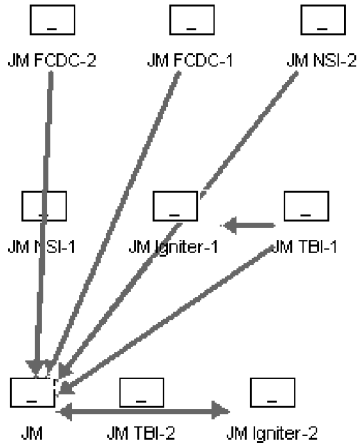
Attitude Control Motor (ACM)



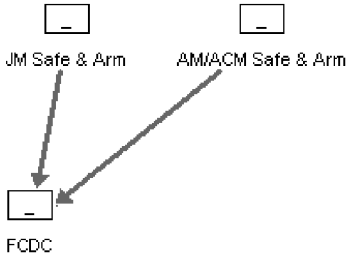
Abort Motor (AM)



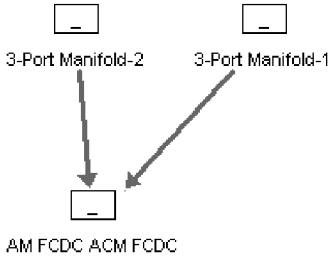
Jettison Motor (JM)



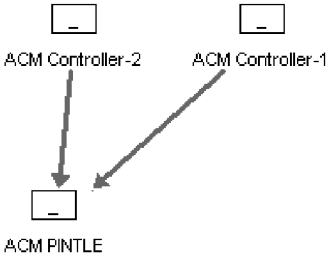
Safe & Arm Components



Manifolds



ACM Controllers



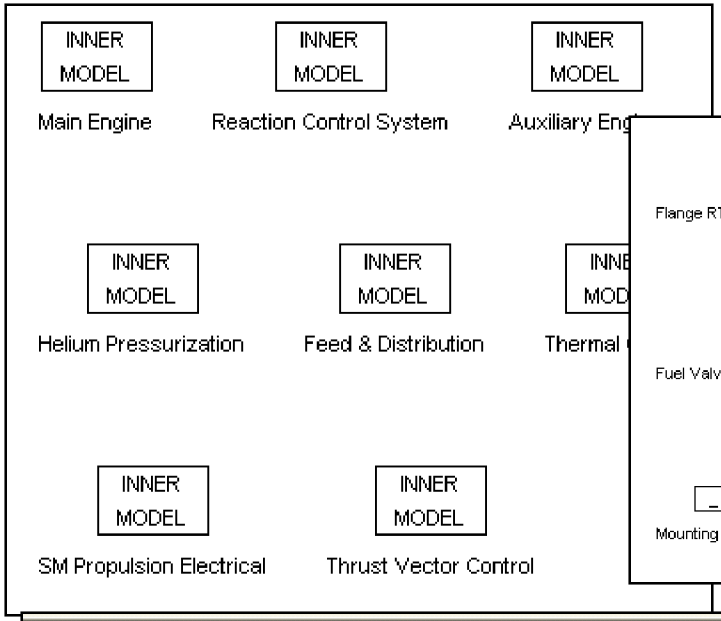
- Numbered multiple instances of components
- Pop-ups on components and connections, with model information and traceability

TBI – Through Bulkhead Initiator
NSI – NASA Standard Initiator
FCDC – Flexible Confined Detonating Cord (a network)

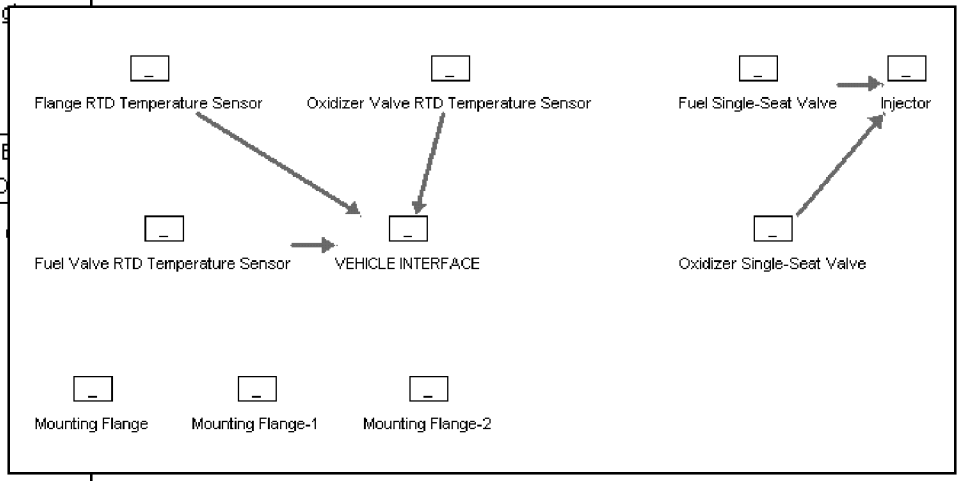
From LAS Case to CEV SM

- Generalized to another Orion case: Service Module (SM) Propulsion
  - PDR data book had updated FMEA/CILs and Hazard Reports for extraction
  - Documents for other subsystems were generally less complete and less mature
- Identified and met new challenges
  - New FMEA/CIL worksheet format, Hazard Report format, new text styles

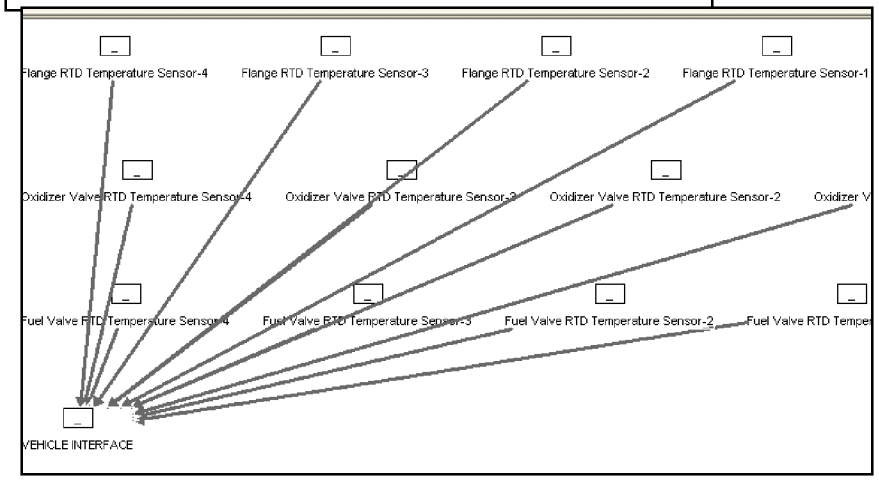
SM Propulsion Case Results



SM Auxiliary Engine Model Visualization (Partial)



RTD – Resistive Temperature Device



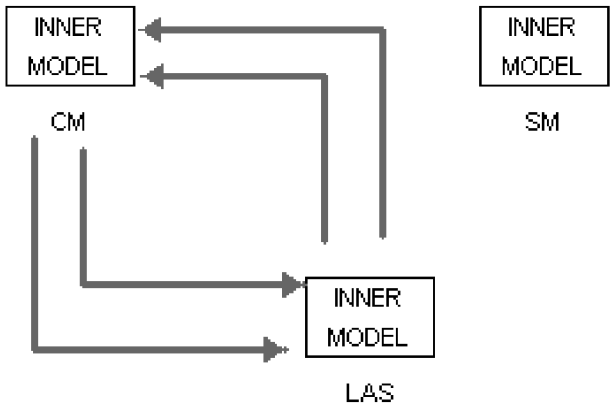
SM Reaction Control System (RCS) Model Visualization (Partial)

Model Construction

- Hazard Identification Tool (HIT) automatically processes extracted XML
  - Uses component hierarchy to define model hierarchy and inner models
  - Generates component-connection models, using ontology to identify types of components, connections and flows on connections
  - Associates with components and connections: functions, hazards, failures and traceability information
- Visualization for Safety personnel
- XML output for model information reuse

LAS Information Extraction

- Top-Level Model from IIRD Document



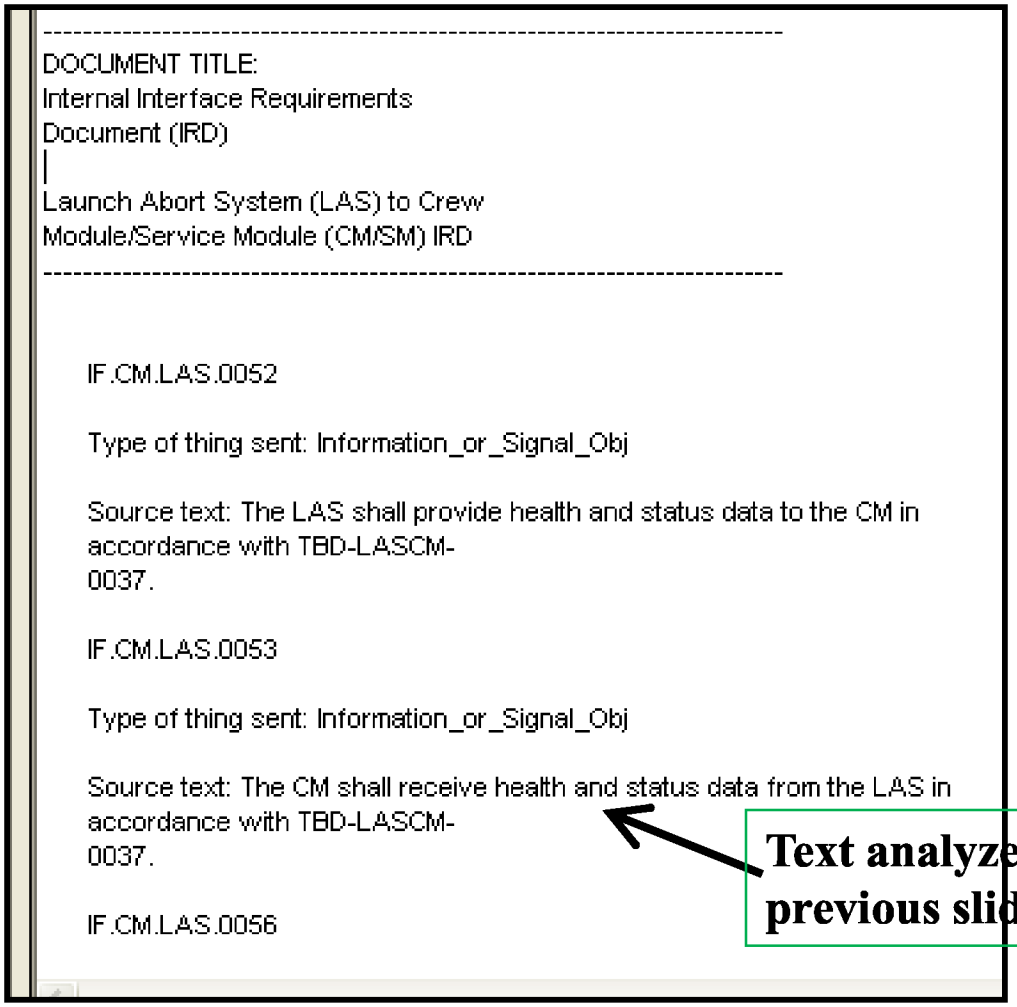
- Text extraction and screening against the ontology

"The CM shall receive health and status data from the LAS in accordance with TBD-LAS- CM-0037."

((:SENDER "LAS" :MATCHES (#<CONCEPT-CLASS "Abort_System >))
(:RECEIVER "CM" :MATCHES (#<CONCEPT-CLASS "Aerospace_System">))
(:OBJECT "DATA" :MATCHES (#<CONCEPT-CLASS "Information_or_Signal_Obj">))
(:VERB "receive" :MATCHES (#<CONCEPT-CLASS "Receive">)))

Pop-up Documentation for Connections

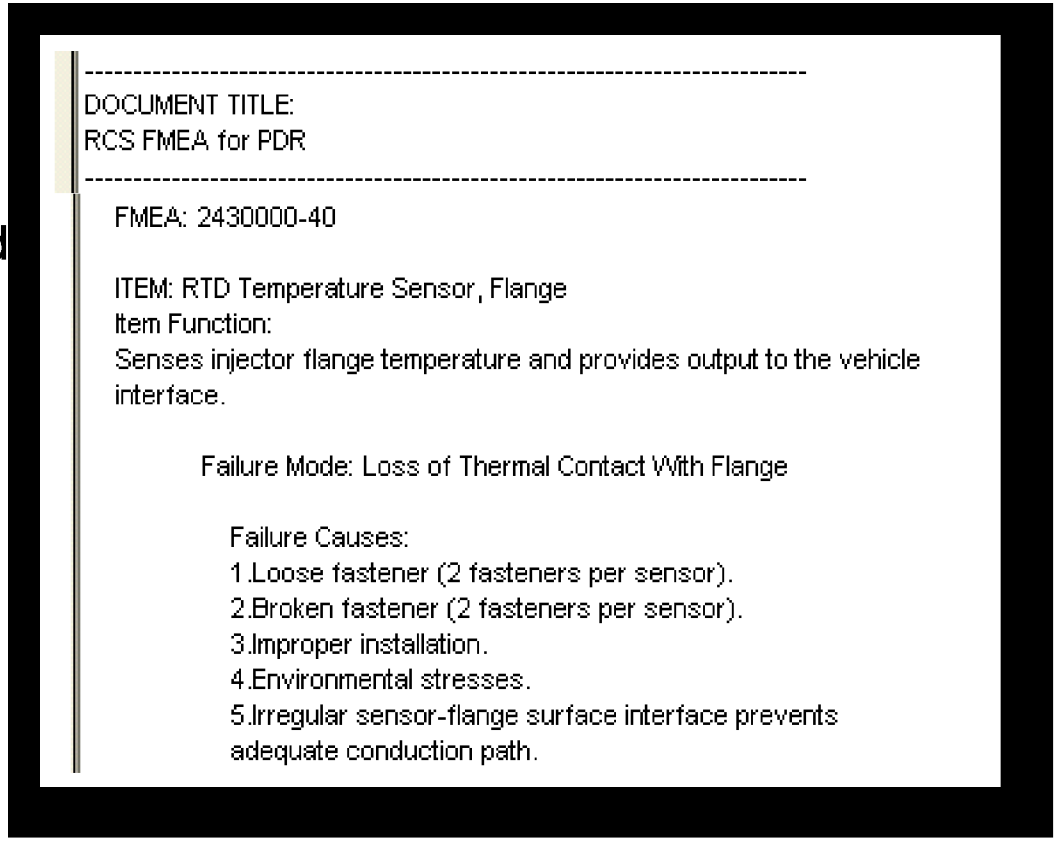
- **Box pops up when user clicks on connection arrow**
- **Information**
  - **Document Title**
  - **Requirement number**
  - **Type of thing sent : Info/Signal**
  - **Source Text**
- **Multiple interface requirements describe this connection**
  - **Provide version**
  - **Receive version**



A connection from the LAS to the CM

Pop-up Documentation for Component

- **Box pops up when user clicks on component**
- **Information**
  - FMEA Document Title and FMEA worksheet number
  - Item Name: …**Sensor**…
  - Item Function: **Senses … temperature** and **provides output to the vehicle interface**
  - Failure Modes: Loss of Thermal Contact…
  - Causes for each failure mode
  - Sub-component: Fastener



Component: temperature sensor for a flange

Evaluation by Safety Engineer

- Evaluation session with K. Chen, responsible for Orion avionics safety
- Positive Reactions to Visualization
  - Helps analyst look for missing information in the documents in an organized and efficient way
  - Helps analyst check if hazard path is correct and whether fulfills requirements
  - **Combining extractions from IIRDs, FMEAs and detailed Hazard Analyses can help build a complete picture and identify missing and inconsistent information**
    - Identify things appearing in the FMEA but not Hazard Analysis and vice versa
    - Looks forward to taking this combined information to his safety engineer and the Orion contractor
  - References to source documents are helpful
  - This tool should interest NASA headquarters.
- K. Chen has provided detailed LAS System Hazard Reports for model extraction to get the combined picture

From FMEA to Hazard Analysis

- Extraction from Hazard Report text for the Hazard Identification Tool (HIT) models and visualizations
- Extractions from Orion Hazard Report: “Failure to Fire Electrically Controlled Pyrotechnics results in Loss of Crew/Loss of Mission”
  - Cause B: Avionics/Electrical Failure
  - Cause B description example (4 causes are listed)
    - “A failure in the Test Port Flight Cap prevents power or redirects power through a short circuit causing no power to reach the NSI.”
  - Cause B controls example
    - “RIU Test Port Flight Cap is designed to prevent shorts of one or more firing lines.”

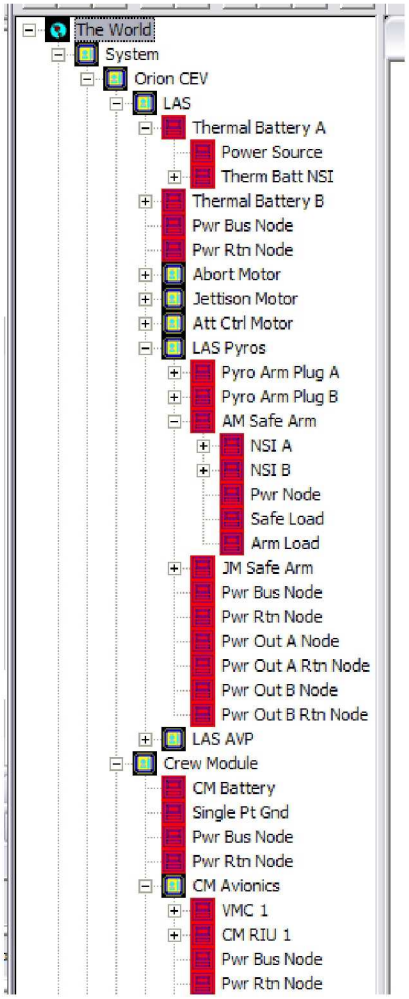
Hazard Report Extraction Examples

- Extraction from Cause Description and Cause controls
- Components, sub-components, connections, entity in Path
  - "RIU Test Port Flight Cap, NSI, firing lines, power"
  - Others: "EPS, MBSU, PEC power supply, PEC firing circuits, PEC capacitor banks, Flight Plug"
- Faults and failures
  - "RIU Test Port Flight Cap failure"
  - "Short circuit, short" (or sneak circuit, fail open, race condition)
  - "Prevents power, redirects power" (or not deliver energy)
  - "No power reaches NSI"
  - Others: "fails to command"

XML Output for Model Reuse

- XML file output of model information and traceability for use in other tools
  - Components, connections, and other model properties
- XML output function uses an easily changed specification
  - Accommodates changes in the model structure or output properties
- XML output for LAS pyrotechnics model delivered to Triakis

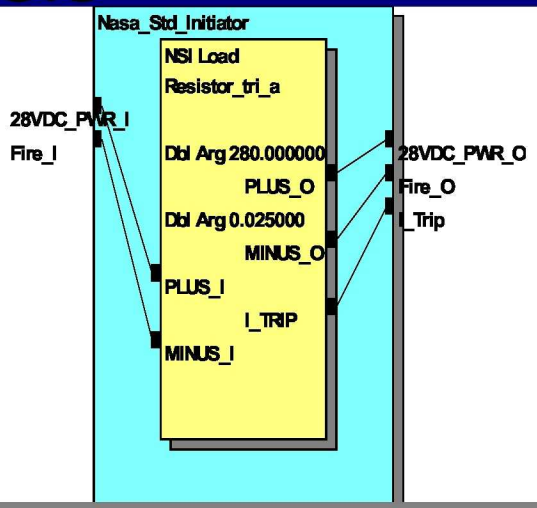
Virtual System Integration Lab (VSIL) LAS Models



- LAS VSIL part tree

Example NSI part

- Connections, interfaces and Input / Output
- Inner models
- Functions (Requirements)
- Internal variables
- Failures



Class Name	Nasa_Std_Initiator
Parts: Class/Name	
Resistor_tri_a	NSI Load
Input Signals: Name/Type	
28VDC_PWR_I	Sig Thev
Fire_I	Sig Thev
Output Signals: Name/Type	
28VDC_PWR_O	Sig Thev
Fire_O	Sig Thev
I_Trip	Sig Bool
Initiate	Sig Bool
Requirements	
1. The NSI shall initially be READY to fire. 2. The NSI shall send out the Initiate signal upon receipt of a FIRE signal greater than 7VDC @ 25mA is received. 3. The NSI shall change state to FIRED following FIRE event. 4. Once FIRED, the NSI shall not change states.	

Example LAS Pyro Nominal Test Results

LAS Pyro Nominal Test Results

Test 1: LAS Pyro Safe/Flight Plug Tests

Step 1a. Verify Safe/Flight Plug Initial State == SAFE
  Initial Plug A Status == SAFE: +++ PASS +++
  Initial Plug B Status == SAFE: +++ PASS +++

Step 1b. Verify Safe/Flight Plug output voltage <= 1.0
  Plug A output voltage == 0.187484: +++ PASS +++
  Plug B output voltage == 0.187484: +++ PASS +++

Step 1c. Change Safe/Flight Plug State to FLIGHT
  New Plug A State == FLIGHT: +++ PASS +++
  New Plug B State == FLIGHT: +++ PASS +++

Step 1d. Verify Safe/Flight Plug output voltage >= 24.0
  Plug A output voltage == 27.996068: +++ PASS +++
  Plug B output voltage == 27.996068: +++ PASS +++

Step 1e. Change Safe/Flight Plug State to SAFE
  New Plug A Status == SAFE: +++ PASS +++
  New Plug B Status == SAFE: +++ PASS +++

Step 1f. Verify Safe/Flight Plug output voltage <= 1.0
  Plug A output voltage == 0.205305: +++ PASS +++
  Plug B output voltage == 0.205305: +++ PASS +++

Test 1 Final Result: +++ PASSED +++

Test 2: LAS Safe/Arm Valve Tests

Step 2a. Verify Safe/Arm Valve Initial State == SAFE
  Abort Motor Valve Status   == SAFE: +++ PASS +++
  Jettison Motor Valve Status == SAFE: +++ PASS +++

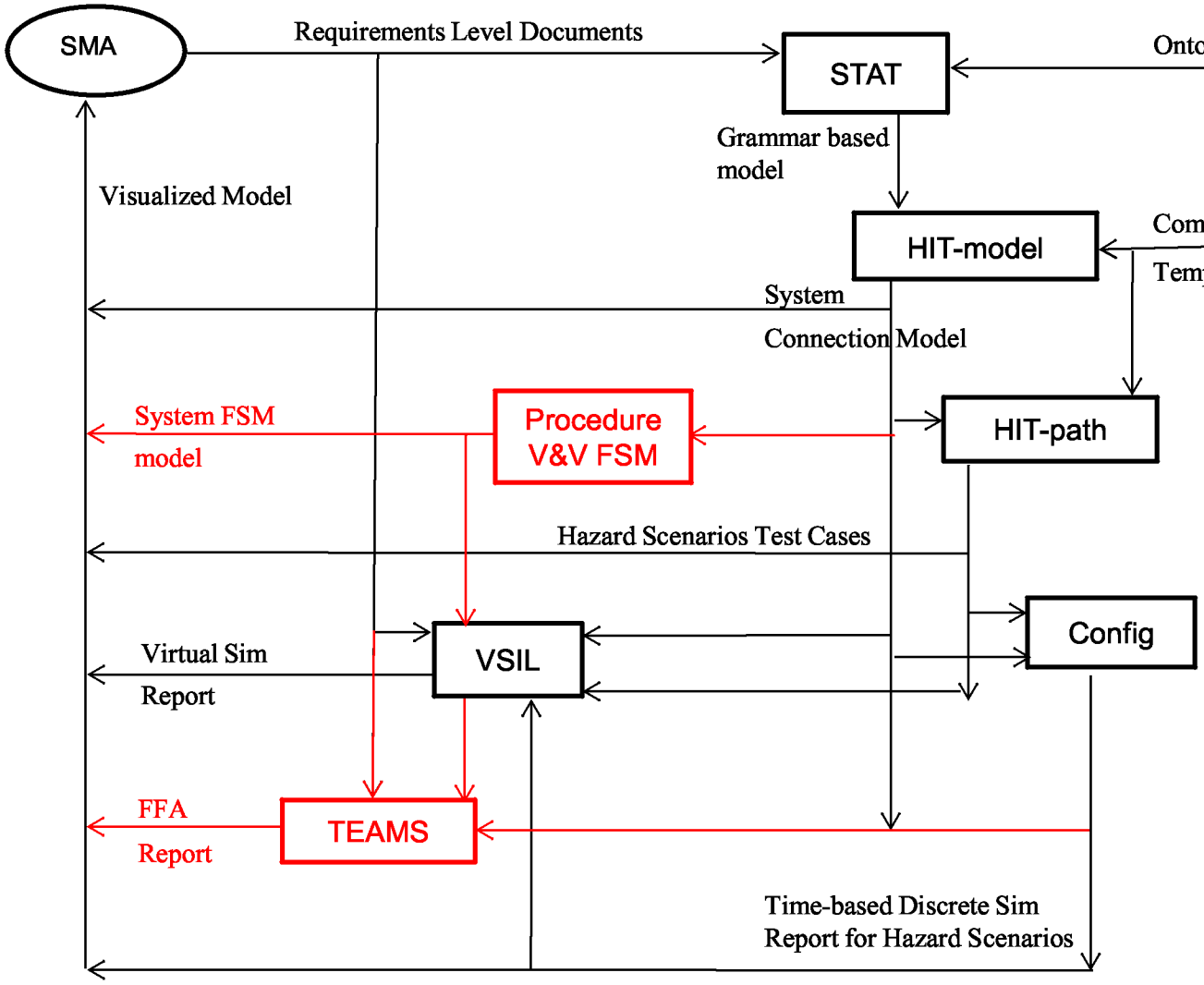
Step 2b. Setting: Command SA Valves to ARMED State
  Abort Motor Valve Status   == ARMED: +++ PASS +++
  Jettison Motor Valve Status == ARMED: +++ PASS +++

Test 2 Final Result: +++ PASSED +++

HIT Models for Path Analysis

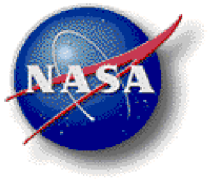
- Hazard Identification Tool models are being enhanced for HIT-path analysis of LAS pyrotechnics paths and dependencies
  - Component mode transitions that are actions with enabling or disabling conditions (e.g., energy, power, percussion)
    - Most LAS operations of concern are mode transitions rather than continuous actions occurring within operating modes
  - Variable properties for entities transferred across connection paths (e.g., command signal values)
- A simplified LAS pyrotechnics model was constructed to test these new capabilities
  - Templates for Pyrotechnic Devices, Pyro Event Controllers, Initiators, Power Supplies, Safe and Arm Devices

Model Reuse Study



Model output for:

- Virtual System Integration Lab (VSIL)
- Finite State Machines (FSMs)
- Functional Fault Models for Testability Engineering and Maintenance System (TEAMS)

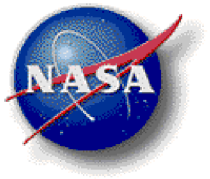


Reusable Model Information

- Component hierarchy and component-connection architecture
  - System modes
  - Configurations and phases
- Functions and actions of components
- Component modes/states and transitions
  - Operating and failure modes
  - State transitions and triggers
- Faults and hazards
  - Disabled functions, actions and transitions
- Instrumentation and key value constraints

Findings/Recommendations

- Visualization can help SMA personnel
  - Overview and drill down to review large documents
- Most useful documents are IIRDs, FMEAs, Hazard Reports at PDR
  - Pre-PDR documents are not mature enough
  - Extraction from requirements, structured text descriptions, structured worksheets and tables
    - PowerPoint charts and schematics are not promising formats for extraction
- Standard requirements formats for model generation could help both authors and modelers
- Model extractions can be reused for FSMs and TEAMS models



Planned Capability

- Situations where these tools can be applied
  - Automatic extraction of Information for model development in aerospace programs and projects (Orion, Altair & others)
    - System components connections, interfaces, dependencies
    - Functions, actions, failures and hazards
    - Modes and states and transitions
    - Auxiliary information such as source text and traceability information
  - Development of low-fidelity early (PDR) models of systems interacting with software and controls
  - Development of visualizations for safety analysis
  - Analysis/simulation of system dependencies and paths of failure causes, effects and hazards
    - Identify scenarios for integration tests

Technical Solutions & Challenges

- Technical Solutions
  - Improved extraction from structured text in more types of documents and document sections
  - More automation of construction of models and visualizations from extracted information
  - Specification files to handle changes in extraction, model construction, and XML model output
- Improvements needed for wider use
  - Support for updating specification files
  - More support for manual interaction in model construction, review and expansion
  - Library of model templates for types of components
    - Methods for mapping model information to templates
  - Support for systematic path analysis